

Civil Action No. H-01-3624  
(Consolidated)

**UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF TEXAS  
HOUSTON DIVISION**

United States Courts  
Southern District of Texas  
FILED

FEB 12 2002

Michael W. Milby, Clerk

MARK NEWBY, et al., Individually and On Behalf of All Others  
Similarly Situated,

*Plaintiffs,*

- against -

ENRON CORP., et al.,

*Defendants.*

**REPORT OF ARTHUR ANDERSEN, LLP ON DOCUMENT  
IDENTIFICATION, COLLECTION, RESTORATION, AND  
RETENTION**

275

## TABLE OF CONTENTS

	<u>PAGE</u>
REPORT OF ARTHUR ANDERSEN, LLP ON DOCUMENT IDENTIFICATION, COLLECTION, RESTORATION, AND RETENTION .....	1
I. SUMMARY .....	1
II. BACKGROUND .....	4
III. WORK PAPERS .....	4
A. Identification .....	4
B. Collection .....	5
C. Storage and Security .....	7
IV. DESK FILES .....	9
A. Identification .....	9
1. <u>Identifying Andersen Employees Subject to Document</u> <u>Collection</u> .....	9
2. <u>Physical Locations</u> .....	9
B. Collection .....	10
1. <u>Scope</u> .....	10
2. <u>Collection</u> .....	10
C. Preservation and Security .....	10
1. <u>Box Numbering System and Sacred Sets</u> .....	10
2. <u>Security</u> .....	12
V. E-MAIL .....	13
A. Identification .....	14
B. Collection .....	14
1. <u>E-mail Servers and E-mail Server Backup Tapes</u> .....	14
2. <u>Personal Computers</u> .....	16
3. <u>Removable Media</u> .....	17
C. Storage and Security .....	17
D. Analysis and Review .....	20
1. <u>Existing E-mail</u> .....	20
2. <u>Deleted E-mail</u> .....	20
VI. ELECTRONIC FILES .....	23
A. Identification .....	23
B. Collection .....	23
1. <u>File Servers and File Server Backup Tapes</u> .....	23

PAGE

	2.	<u>Personal Computers</u> .....	24
	3.	<u>Removable Media</u> .....	25
C.		Storage and Security .....	25
D.		Analysis .....	26
	1.	<u>File Servers and Personal Computers</u> .....	26
	2.	<u>File Server Backup Tapes</u> .....	28
	3.	<u>Removable Media</u> .....	29

**REPORT OF ARTHUR ANDERSEN, LLP ON  
DOCUMENT IDENTIFICATION, COLLECTION,  
RESTORATION, AND RETENTION**

Arthur Andersen, LLP ("Andersen") submits this preliminary report on document identification, collection, restoration and retention pursuant to this Court's order dated January 23, 2002. Andersen is still in the preliminary stages of these processes. As a result, this Report is focused upon the primary activities in which Andersen has been engaged: identification, collection and preservation of paper and electronic materials. Although some work on restoration has begun, it is still in the most preliminary stages.

**I. SUMMARY**

Andersen's document process consists of four basic steps: identification of the individuals from whom documents must be retrieved; collection of the documents themselves; recovery of any deleted or destroyed materials; and secure storage of all collected documents. These steps are being performed for four general categories of documents: work papers; desk files; e-mail; and electronic files.

Andersen has constructed and prioritized an evolving list of Andersen individuals from whom documents and electronic media must be collected. Andersen is also identifying physical locations from which paper documents and electronic media must be collected.

Andersen has collected substantial numbers of work papers, desk files, e-mail, and electronic media. Thus far, Andersen has assembled the following:

- Approximately 4,800 official work paper files and reports, including coverage from 1997 through 2001 and additional work papers and reports dating as far back as 1932;

- Approximately 1,500 boxes of desk files from some 235 individuals and common files, with an estimated three million sheets of paper collected;
- Approximately 4,000 server backup tapes, 340 personal computers, 100 gigabytes of Connected Network Backup data, at least 50 Palm Pilots, and more than 300 removable media such as floppy disks, CD-ROMs etc.

In all, Andersen has collected roughly 250 terabytes of electronic data.<sup>1</sup> These quantities of paper and electronic documents are increasing daily, as more and more material is collected.

Extensive efforts are underway to identify and recover deleted material. Andersen believes that many discarded paper documents may be located in the files of other individuals or can be recovered from the computers on which they were created. For e-mails, a comprehensive recovery process is already well underway. A similar recovery process has been started for electronic files other than e-mail.

All collected material is being stored at secure sites. The main storage facility is located in Houston, on a segregated floor at 711 Louisiana Street ("711 Louisiana"). An armed guard is posted outside the facility twenty-four hours a day, seven days a week. Only Andersen's outside counsel, Davis Polk & Wardwell ("DPW") and Rusty Hardin & Associates, and select Andersen personnel have access to the facility via electronic key pass, and even those

---

<sup>1</sup>By comparison, the entire U.S. Library of Congress is estimated to represent between 20 and 100 terabytes of data. A byte is a unit of memory or data equal to the amount used to represent one character. A terabyte is a trillion bytes.



authorized personnel must sign in as they enter. Inside, hard copy and electronic materials are stored in secure rooms, to which only four DPW employees and a building manager (as per building regulations) have a key.

A much smaller amount of paper and electronic material is being temporarily stored by DPW in a secured room at 330 N. Wabash Street, Chicago, Illinois.<sup>2</sup> This room is also guarded 24 hours a day and the keys to that room are held by DPW and the building manager (as per fire regulations). All persons entering the room must sign in and out. If the person entering the room is not associated with DPW, that person must be accompanied by someone from the firm.

On January 28, 2002, DPW and its experts met with plaintiffs' counsel and their experts to discuss the document retrieval and recovery efforts. On January 30, 2002 and February 1, 2002, Andersen opened its document storage facilities in Chicago and Houston, respectively, to inspection by plaintiffs' counsel, their experts, and the Texas Attorney General's office.<sup>3</sup> Counsel and their retained experts were able to examine the facilities and ask questions regarding security and about the collection process.

---

<sup>2</sup>DPW's current plan is to transport all original materials held in Chicago to the Houston facility.

<sup>3</sup>Since the date of plaintiffs' inspection, additional material has been collected in Chicago and is being stored in an additional room under the same conditions as applied to the room viewed by plaintiffs.

This report explains the processes that have been undertaken to date with respect to document and electronic media collection, and the progress that has been made in identifying and recovering deleted material.

## **II. BACKGROUND**

On January 4, 2002, Andersen advised the United States Securities and Exchange Commission ("SEC") and the Department of Justice ("DOJ") that an undetermined number of hard copy documents and e-mails potentially related to Enron had been destroyed or deleted. On January 10, 2002, Andersen similarly advised the public.

As set forth in this report, in response to these issues, additional security measures were adopted to ensure the integrity of materials that had been collected previously by outside counsel in the ordinary course of addressing the litigation and regulatory inquiries. Additionally, various steps were taken to prevent the possibility of any further loss of information, including a firm-wide Andersen directive to preserve all documents, including all forms of electronic media.

Andersen is continuing its efforts to find, restore and preserve any information that had been destroyed or deleted. With regard to deleted e-mails or electronic files, DPW has retained technical experts to obtain and restore the information, and these experts have implemented sophisticated processes to facilitate these tasks. Sections V and VI of this report describe these processes.

### **III. WORK PAPERS**

#### **A. Identification**

A master list of Enron-related work paper files was initially created including work papers for the period 1997 to 2000. The master list included work papers which the engagement team believed existed, but which could not immediately be located. The engagement team then reviewed all Enron job numbers, which are used by Andersen for billing purposes, to confirm that no relevant work papers were overlooked. Non-engagement team Andersen personnel assisted in identifying, listing and collecting the work papers. At the end of this process, all of the lists were merged, and a final master list of work paper files was created.

#### **B. Collection**

Work papers for the period 1997 to 2000 were collected from 3 Allen Center, in Houston, where until December 21, 2001, the Enron engagement team was located, and delivered by City Central Courier to Andersen's offices at 711 Louisiana. Enron-related work paper files for the period 1997 to 2000 also were collected from Andersen's Records Center. The work papers for the year 2001 were not sent at that time because the engagement team was continuing work on those files.

Andersen personnel not on the Enron engagement assisted in document collection and preservation at the direction of outside counsel. Each file was assigned a master file number and the work papers were placed in a secure room on the 16<sup>th</sup> floor of 711 Louisiana.

A library system has been implemented for the work papers. The library was initially staffed by Andersen personnel not on the Enron engagement working at the direction of outside



counsel. At all times during regular business hours, personnel were stationed outside the room where the work papers were stored, and a process for checking out documents was established. Using an electronic version of the master file list, Andersen personnel not on the Enron engagement recorded the name of the person checking out a document and the date that the document was checked out. A slip of paper containing that same information was also placed in the library in place of the checked out document. On January 24, 2002, DPW assumed sole responsibility for the maintenance of the work paper library.

Targeted searches were conducted under the supervision of outside counsel for work paper files which were on the master list but had not yet been located. In late December 2001, outside counsel reviewed the master list maintained by the Andersen personnel, as well as each individual work paper file in the library, to ensure that the work papers had been properly catalogued and stored.

In a number of instances, work papers were made available to certain groups for review, including the SEC, Congressional committee staff members and counsel for the Special Committee of Enron's Board of Directors. Each of these groups visited 711 Louisiana to review Andersen's work paper files. At all times during such reviews by third parties, outside counsel brought the work papers into a conference room, and checked the documents back in at the conclusion of the review. The conference room where outside parties reviewed the documents was locked whenever the outside parties were not present.

When the Enron engagement ended on January 17, 2002, DPW collected all Enron-related work papers for the year 2001. After this collection, master file numbers were assigned

to the 2001 work papers and they were added to the library. The same check out process was used for these new files. Again, outside counsel examined each individual work paper file in the library and verified the accuracy of all entries on the master file list.

In accordance with this Court's January 23 order, outside counsel expanded the scope of the document collection by arranging to collect all Enron-related work papers for all time periods. Accordingly, in January 2002, outside counsel coordinated the collection of all Enron-related work papers, including tax and business consulting work papers, for all available years. These files also were assigned master file numbers and were integrated into the existing work papers library.

For the period 1997 through 2001, outside counsel has secured 1,733 work paper files and reports. Three audit work paper files for this period have not been located, but of these, two files have been partially recreated. Our understanding is that the remaining file has been missing since at least July 2001. We have no reason to believe that these files were destroyed and we are continuing our search. DPW has also secured 3,167 work paper files and reports relating to Enron and its predecessor corporations for audit, tax and business consulting services performed prior to 1997. The earliest report on file dates from 1932. Outside counsel is currently expanding the master file list to include all of the pre-1997 work papers and reports.

### **C. Storage and Security**

As a result of the collection of numerous additional work paper files, the work papers library has been expanded from one room to three rooms. One room houses the set of audit work papers relating to the years 1997 through 2001. The second room contains the audit

work papers relating to the period 1932 through 1996. The third room consists of some additional audit work papers relating to the period 1932 through 1996, as well as Enron-related tax and business consulting work papers dating back to 1997.<sup>4</sup> These rooms are monitored at all times by outside counsel, and outside counsel maintains a master file list. Only four DPW employees possess the keys to the three work papers library rooms.

There is a strict library check out procedure for work papers. DPW may check out documents. Experts assisting with audit review and the Andersen personnel assisting them may also check out work papers for review. Any files checked out by this team must be returned to the work papers library at the end of the business day. Other Andersen personnel requiring access to the documents may review them, but only in the presence of outside counsel. Under no circumstances may any non-DPW personnel remove a work paper file from the 16<sup>th</sup> floor.<sup>5</sup> If Andersen personnel wish to obtain a copy of any document contained in the work papers library, that person must submit a request to DPW, which will then provide a copy.

To date, because of the extraordinary demand made for access to the original work papers, they have not yet been copied in their entirety. Plans for copying entire sets of the papers are in the process of implementation.

---

<sup>4</sup>DPW is now in the process of compiling tax work papers for prior periods, extending back to the mid-1980s.

<sup>5</sup>Large scale copying has been done to date through outside vendors, not located at 711 Louisiana. Going forward, DPW is contracting with a service that will perform all copying on the 16<sup>th</sup> floor.



#### **IV. DESK FILES**

##### **A. Identification**

###### **1. Identifying Andersen Employees Subject to Document Collection**

The first task involved identification of the specific Andersen employees subject to document collection. Outside counsel used a variety of sources to identify persons who potentially have documents responsive to the subpoenas received and lawsuits filed. These sources included personnel lists, floorplans, telephone directory lists, and billing records. These lists were initially focused on Houston based audit work, but have been expanded to include non-audit work and non-Houston based work in all categories. The identification of persons who performed non-Houston based Enron-related work is not complete. In addition, DPW has not identified individuals who billed time to Enron-related matters prior to 1997.

###### **2. Physical Locations**

Collections have been made from the following locations: a) Andersen's former offices at 3 Allen Center, Houston, Texas; b) Andersen's offices at 711 Louisiana Street, Houston, Texas; c) Andersen's offices at 33 West Monroe Street, Chicago, Illinois; d) Andersen's offices at 111 S.W. Columbia Street, Portland, Oregon; and e) Andersen's offices within Portland General Electric at 121 S.W. Salmon Street, Portland, Oregon. In addition, documents are being or will be collected from other Andersen offices.

Finally, in certain instances, DPW staff have traveled to individuals' personal residences or met with them at their clients' offices, in order to ensure the timely collection of relevant documents.



## **B. Collection**

### **1. Scope**

The initial collection was focused on documents dating from 1997 through the present. The collection subsequently has been expanded to include all pre-1997 Enron-related documents. This expanded collection effort has required the retracing of steps from the earlier collection. However, the search for pre-1997 documents now continues concurrently with all other collection efforts and priorities.

### **2. Collection**

Procedures were implemented to ensure an orderly and comprehensive collection. The collection process is fully documented. Outside counsel, with the assistance of non-legal personnel, reviews the relevant Andersen employee's documents and determines whether responsive documents may be located in other locations. All original documents are secured and removed for copying.<sup>6</sup>

## **C. Preservation and Security**

### **1. Box Numbering System and Sacred Sets**

DPW has instituted a comprehensive system to segregate, preserve and protect the approximately 1,500 boxes of desk files collected so far. Upon collection, each box is

---

<sup>6</sup>DPW attorneys are assisted by legal assistants and clerks to aid in the administrative aspects of the collection effort by performing such tasks as logging boxes, ensuring the security of the storage rooms and assisting in the copying process. In late January, DPW retained Decision Strategies, a consulting group which provides additional personnel to aid in these tasks. *See Exhibit A (Decision Strategies profile).*

assigned a number and the information concerning its collection is input into a log. Each box is then sent for copying. Once a box is returned from the copy center, the originals are immediately placed into one of five secure "sacred rooms" maintained by DPW, where they are ordered sequentially. While the originals remain secure in the sacred rooms, the copies are packaged and prepared for overnight transport to Cypress Technology and E-Business Center ("CTEC"), a division of Andersen, which is converting paper and electronic documents to a form in which they can be reviewed by attorneys.<sup>7</sup>

Once the copies have been electronically scanned by CTEC, they are sent to DPW's New York office. At all times, the originals remain securely housed in the Houston "sacred rooms," while a duplicate "sacred" set is created in New York. At the close of the process, there will be two complete "sacred" sets, in addition to an electronically scanned version, thus providing maximum assurance that the current state of documentation is being entirely preserved. In addition, DPW will review samples of CTEC's electronic scanning work to confirm its accuracy and completeness.<sup>8</sup>

It should be noted that during the initial stages of the document collection, certain original documents were still being used by Andersen employees in ongoing work on Enron-related projects. In such cases, two copies of all original documents were made and the

---

<sup>7</sup>DPW has retained CTEC for the scanning of documents on more than 50 occasions over the last few years, and they have scanned over 30,000,000 pages for DPW over that time. A copy of the CTEC profile is attached as Exhibit B.

<sup>8</sup>DPW expects to retain a new outside vendor that will perform the scanning services that to date have been performed by CTEC, and to provide these services in Houston.

originals were then returned to the employee while outside counsel retained both duplicates.

This process ended when Andersen's relationship with Enron ceased, and from that point forward, no originals were returned to employees.

In order to ensure the swift duplication of the large boxes being filled during each day of collection, DPW originally engaged two copy centers. The entire process of sending boxes to the copy centers and receiving the originals and copies back has been documented and tracked. DPW has also implemented sample review procedures to monitor the accuracy and quality of the copying.

## 2. Security

The entire document storage complex in Houston is contained within the secure area on the 16<sup>th</sup> floor of 711 Louisiana. Outside the entrance, a uniformed off-duty officer of the Houston Police Department stands guard seven days a week, twenty-four hours a day. Access to the floor is also regulated by electronic identification cards. Although the cards allow entry to the general areas of DPW's workspace, the actual rooms that house the documents and electronic media are kept under lock and key, to provide an additional layer of security. Keys to these rooms are held by only four DPW employees, and access is thoroughly maintained and guarded by these individuals.

The document collections in other cities, while much smaller in scale, are treated with similar measures of security. In Andersen's Chicago offices, the collected documents are sequestered in a room to which only a DPW attorney and a building manager (as per fire regulations) have the key. Documents are also being collected from other offices and secured



DPW's New York office, where two rooms have been allocated for security and processing purposes.<sup>9</sup> These documents have been transferred to Houston periodically.

## **V. E-MAIL**

Along with paper documents, electronic material constitutes a significant component of the broader document collection process. One estimate found that DPW has so far collected roughly 250 terabytes of electronic data. This amount of information is equivalent to about 78 billion pages of printed documents.

To assist in the collection and processing of electronic information, outside counsel has retained technical specialists. Ibis Consulting, Inc. ("Ibis") is a leading firm in the field of electronic collection, storage, recovery and analysis. The founder and President of Ibis, Jay McNally, has been working closely with outside counsel in Houston. *See* Exhibit C (resume for Mr. McNally). The Ibis team is deployed in other U.S. cities as well, and is processing data collected in Houston and elsewhere. Andrew Rosen of ASR Data Acquisition and Analysis, LLC ("ASR"), a leading expert in the field of computer forensics, has also been retained. *See* Exhibit D (resume for Mr. Rosen). Mr. Rosen and his team are responsible for recovering data from personal computers ("PCs"), servers, and personal digital assistants ("PDAs"). Finally, Lee Tydlaska of Computer Conversions has been retained to restore server backup tapes. *See* Exhibit E (resume for Mr. Tydlaska).

---

<sup>9</sup>In the past, DPW's New York and Menlo Park offices have been used as temporary storage locations, as has Andersen's Portland Office. At all times, DPW personnel controlled access to the storage areas in these temporary locations.



## **A. Identification**

The process of identifying the universe of Enron-related e-mail has been similar to that for paper desk files. The starting point is identifying individuals through use of a collection list.

## **B. Collection**

### **1. E-mail Servers and E-mail Server Backup Tapes**

E-mail is stored on various media. Because Andersen uses a networked e-mail system, the principal location of e-mail is on centralized computers called servers. Mail servers are separate from file servers, which process and store word processing documents, spreadsheets, and other electronic files. Each e-mail server contains the e-mail mailboxes for a group of users; that machine is called their home server. For the e-mail system used by Andersen, Lotus Notes, it is possible to collect the existing e-mail mailbox for an individual by simply copying an image of that mailbox from the relevant server.

In November, images for about 90 mailboxes were either copied real-time from e-mail servers or were taken from backup tapes. Images of additional e-mail mailboxes are copied as additional individuals are identified as having worked on Enron-related matters.

In addition to the e-mail servers themselves, there are several other sources of e-mail: e-mail server backup tapes; personal computers; and removable media. E-mail servers are periodically backed up – that is, copied – in case the physical computer fails or is damaged. At Andersen, the data from a backup is stored on magnetic computer tape. These e-mail server backup tapes are normally stored for a specific period of time, after which they are reused, and new backup data is rewritten over the old backup data. Backups are of two types: incremental

and full. A full backup copies all of the information on a server. An incremental backup, sometimes called a differential backup, copies only changes that have been made to the server since the previous backup. If a server were disabled after only an incremental backup, the data would be restored by combining the last full backup with any subsequent incremental backups. At Andersen, generally, full backups of e-mail servers were performed daily, except on Sundays when no backup was performed.

E-mail server backup tapes are stored differently according to their type. In Houston, daily tapes are stored on site for approximately 30 days. After that, they are placed in a tape recycle bin and reused. Weekly backup tapes are stored for approximately 30 days at an off-site facility, Iron Mountain, Inc.<sup>10</sup>

DPW collected e-mail server backup tapes from various locations, including the Iron Mountain facility. DPW also conducted searches of all Houston offices of engagement team members, their individual and common filing cabinets, their storage spaces, and the Houston technology work spaces. In addition, e-mail server backup tapes are being secured for collection in other Andersen offices.

To date, approximately 2,000 e-mail backup server tapes, containing about 160 terabytes of data, have been collected.

---

<sup>10</sup>The reuse of server backup tapes has been suspended.

## 2. Personal Computers

In addition to backup tapes, personal computers ("PCs") provide a source of e-mail data. Although Andersen relied primarily on its servers for e-mail, the e-mail software program used by Andersen, Lotus Notes, can store a replica copy of each mailbox on the local hard drive on the PC.

In November, technicians copied the hard drives of certain computers in Houston. The data were written onto a server, and over the following few days were downloaded onto data tapes. However, because the physical hard drive may contain forensic data that is not available on a copy, beginning on January 7, 2002, hard drives and/or entire personal computers were also collected. Efforts have also been made to recover PC hard drives from people who have left the firm.

Personal computers were also collected by outside counsel in other parts of the country, where Andersen employees were traveling for business purposes. Personal computers were also gathered from employees who were based in Houston but are now based in other offices around the country. In all, approximately 340 personal computers have been collected. As PCs are brought to Houston, they are logged into a separate index. The PCs currently in Houston alone contain approximately three terabytes of data, some portion of which is e-mails. These numbers are increasing daily, as personal computers are collected in other cities.

Andersen also routinely backs up certain electronic files from end-user personal computers using a system called Connected Network Backup ("CNB"). Consequently, CNB

data may include e-mail mailboxes located on PCs. To date, this data is being collected and analyzed in the same way as for CNB data containing electronic files.

### 3. Removable Media

In addition to e-mail servers and personal computers, removable media may contain e-mail. Examples of removable media include floppy disks, CD-ROMs, DVDs, swappable hard drives, JAZ cartridges, and ZIP cartridges. These media were collected during the searches for desk files, and in searches of common areas and of the computer technology service areas.

Each piece of removable media was individually logged into a database. At last count, the collected removable media numbered about 830, or approximately 40 gigabytes of data. The quantity of e-mail contained on those media has not yet been determined.

### **C. Storage and Security**

DPW's main data storage facility is located in Houston. The electronic media storage facility is on the same floor, and subject to the same security measures, as the document collection materials. The electronic data room is accessible by only four members of the DPW team.

Inside the data room, each server, server drive, personal computer, server backup tape, floppy disk, CD-ROM, DVD, and PDA (such as a Palm Pilot) is individually logged into a database. DPW staff label each item with an individual identifier and place it into a plastic bag. Staff then seal the bag and sign across the seal.<sup>11</sup> When an item must be removed from

---

<sup>11</sup>Some items, such as server racks, are too large to place into plastic bags. A seal is placed across the doors to these racks.



the data room for any reason – for instance, to perform analysis – it must be checked out of the database to the person who receives the medium. The seal is then broken. The party receiving the medium, such as Ibis or ASR, will then keep their own log documenting chain of custody. Ibis or ASR then logs the item and records its serial number, as well as any serial numbers on the system's components as it is disassembled for analysis. The technician also documents exactly what procedures are performed on a given medium, as well as any unusual findings. The medium is then reassembled, if necessary, and returned to the data room. It is checked back into the database, placed into a plastic bag, and re-sealed.

As described below, some analysis of e-mail is being performed by CTEC. The e-mail media at CTEC, none of which is original, is stored in a locked media box. The only keys to this box are kept by a few data librarians. The locked box itself is stored in the CTEC server room, which is the most secure part of the CTEC facility. Both doors to the server room are protected by both proximity card readers and hand-geometry scanners. Server-room access is granted only to necessary technicians. CTEC itself is protected by proximity card readers for building access and required sign-in for all visitors.

Other analyses are being performed at the Ibis headquarters in Providence, Rhode Island. Outside counsel has inspected and approved the security protocols at Ibis. These include: a twenty-four hour armed guard; a sign-in requirement for all visitors; electronic passkey access for employees; separate security for data rooms, to which only four Ibis technicians have access; and electronic security for all computer systems.

From time to time, media must be transported. Current procedure allows for transportation of original media only by ground transportation, accompanied by DPW or Decision Strategies staff. However, copies of media may be transported by courier.

In order to minimize the need for secure transportation of original media, data analysis laboratories will be assembled in Houston. One of these, for ASR, has already been assembled. It is separately secured with a lock, for which only ASR carries the key. The other two laboratories will be similarly secured. As mentioned above, both Ibis and ASR maintain their own chain of custody records. No original media are stored in either of the data analysis laboratories, but are stored in the data storage room maintained by outside counsel.

Transportation also occurs from various cities to CTEC, and from CTEC to DPW's New York office. Under current policy, none of the media handled by CTEC is original. Therefore, it may be transferred either physically by Federal Express or electronically to New York through a secure FTP connection. Non-original data is sometimes also transferred to CTEC from Andersen offices via Andersen's internal network.

#### **D. Analysis and Review**

##### **1. Existing E-mail**

Two types of e-mail are subject to analysis: existing e-mail and deleted e-mail. Existing e-mail is processed in a manner similar to paper desk files. Existing e-mail mailboxes are simply converted by CTEC into Tagged Image File Format ("TIFF"), which can be read on a computer. These images are then transported, either electronically or by Federal Express

delivery of CD-ROMs or DVDs, to DPW. The process of converting and reviewing existing e-mails is continuing.

DPW will review samples of existing e-mails to ensure the accuracy and completeness of the conversion process. A random sample of TIFF images will be compared for consistency with the Lotus Notes files. Each Lotus Notes e-mail message in the sample will be compared to its image, and each attachment in the sample will be opened to ensure that it has been accurately imaged along with its cover e-mail message.

## 2. Deleted E-mail

Analysis of deleted e-mail involves comparison of an existing mailbox and an earlier version of that same mailbox taken from e-mail server backup tapes. The contents of some deleted e-mails may be restored from the backup tape. Deleted e-mail that has successfully been recovered can then be converted to TIFF format and sent to New York for review in much the same manner as existing e-mail. DPW is then able to review the contents of a deleted e-mail in order to determine whether the e-mail concerned an Enron-related matter. DPW must then review these Enron-related materials to determine whether copies have been retained elsewhere, or in other forms (i.e. hardcopy, disks, etc.). This process is not yet complete.

In order for deletion analysis to continue apace, it is necessary to continue to restore e-mail server backup tapes. This process is comprised of three stages. First, the tape's electronic label is read in order to determine the server and the backup date. This step determines whether a tape was used to back up a particular e-mail server. Second, the tape is



scanned to create an index of its contents. This step detects whether the tape contains the mailbox of specific individuals. Third, if the tape contains files of a person on the collection list, the tape is restored so its contents can actually be read. During the restore process, two copies are made. One copy is made on another backup tape, while a second copy is written to a PC hard drive.

Ibis is currently scanning tapes at its home office in Providence, Rhode Island. Going forward, Lee Tydlaska of Computer Conversions has been retained to restore server backup tapes. Initially, CTEC was retained to perform the e-mail analysis. (Attached as Exhibit F is a copy of a CTEC report that describes CTEC's procedure for performing the analysis.) However, after January 4, 2002, Ibis was asked to monitor the analysis undertaken by CTEC, and Ibis is in the process of doing so. Ibis staff have visited the CTEC facility. Ibis is comfortable with the general approach outlined by CTEC. Moreover, Ibis will perform a random-sample review of CTEC's deletion analysis as it is completed.

In addition to the deletion analysis performed on e-mail server backup tapes, forensic analysis of actual servers, personal computers and removable media is in progress. Deleted material, including but not limited to e-mail, is recoverable through a variety of forensic techniques. Andrew Rosen of ASR Data Acquisition, Inc. is conducting this process. Initially, ASR is in the process of performing bit-level captures of server drives, PC hard drives, and removable media.<sup>12</sup> A bit-level capture copies all the data from a medium in an exact form, so

---

<sup>12</sup>One software program that ASR employs, Storage Media Archive and Recovery Toolkit ("SMART"), was developed by ASR. SMART functions similarly to a standard and  
(continued...)



that forensic techniques may be applied to the copy without risk of damage to the original medium. Those techniques include, but are not limited to: detection of file fragments; analysis of unallocated space; analysis of "pointers" to files, such as desktop shortcuts; examination of Microsoft Windows registries; detection of whether file-wiping software was used; analysis of machine usage through log files and the like; analysis of Microsoft Windows swap files for virtual memory; and analysis of print spoolers. Bit-level captures will be performed on all media. Full forensic workups will then be ordered for all warranted media.

Finally, it should be noted that while computer users have been receiving copies of their hard drives to enable them to continue working, the copying process is performed in such a way as not to affect the forensics on the original hard drive, which is retained by outside counsel.

## **VI. ELECTRONIC FILES**

Other than e-mail, the major category of electronic data is electronic files. These include substantive files such as word processing documents, spreadsheets, and presentations. Electronic files are organized and stored in a manner distinct from e-mails, and the collection and analysis of such files has differed accordingly.

---

<sup>12</sup>(...continued)

well-known program called "dd," except that SMART works in a graphic environment. The program dd is widely used and is available in the public domain. In addition, ASR uses three widely-used algorithms to verify and authenticate the result generated by SMART. Ibis is aware of SMART and is comfortable with its use.

## **A. Identification**

For all individuals who have had their desk files and e-mails collected, outside counsel is also collecting electronic files.

## **B. Collection**

### **1. File Servers and File Server Backup Tapes**

The vast majority of the Enron engagement team had their primary offices at 3 Allen Center in Houston. The home file server for these engagement team members was housed physically at that facility. The rest of the Houston engagement team, and after the move from 3 Allen Center, the entire engagement team, was located at 711 Louisiana, where their home directories were located on two servers. The physical drives from all three servers are now in the custody of DPW.

File servers, like e-mail servers, are regularly backed up onto computer tapes. Backups are performed in order to preserve data in case of damage to, or failure of, a server machine. We understand that for file servers, full backups are performed in Houston each Saturday, while incremental backups are performed daily. The incremental backups are stored for approximately 30 days on site. The weekly full backups are stored off site for approximately 30 days. One weekly backup per month of tax servers is stored off site for one full year.

All available file server backup tapes have been collected from the Houston office. Outside Houston, file server backup tapes are also in the process of being collected. For all identified individuals who participated in the Enron engagement, the home directory of that

individual is located on a particular server, and all the file server backup tapes for those servers have been, or are being, sequestered and secured. This process is underway in various Andersen offices.

In total, more than 4,000 server backup tapes have been collected and secured, many of which are file server backup tapes (the remainder are e-mail server backup tapes). Together, these tapes hold approximately 200 terabytes of data.

## 2. Personal Computers

Although electronic files are primarily stored on central servers, they also reside on personal computers. Electronic files on personal computers may differ from versions on the central server or may be entirely unique. The PC collection process is described above. *See supra* at 16-17. These devices contain approximately three terabytes of data, some of which represents electronic files.

We understand that Andersen routinely backs up certain electronic files from end-user personal computers using a system called Connected Network Backup (CNB). CNB data for Andersen offices in the United States is stored in Chicago, Illinois and Sarasota, Florida. Altogether, approximately 23,000 CNB files, constituting about 233,000 pages of TIFF images, have been sent to New York for review. CNB collection is continuing.

## 3. Removable Media

Removable media — such as floppy disks, CD-ROMs, DVDs, JAZ and ZIP cartridges, and microcassettes — may contain electronic files, just as they may contain e-mail. These have been collected in the manner described above. In addition, outside counsel has



repeatedly searched computer technology service spaces in Houston in search of removable media. In all, about 830 pieces of removable media have been collected, representing approximately 40 gigabytes of data.

One category of removable media that pertains to electronic files, but generally not to e-mail, is PDAs, including Palm Pilots and similar devices. To date, DPW has collected about 50 PDAs in Houston alone. Collection of PDAs is continuing in the same manner as other removable media.

### **C. Storage and Security**

Media containing electronic files are stored in the same manner as media containing e-mail, and with the same comprehensive security measures employed in safeguarding the desk files and work papers.

PDAs are also stored in the data room. They are kept in individual plastic bags, like the other media, but are not currently sealed because the recharging procedure described below requires frequent access. PDAs do not use rotating magnetic memory devices such as hard drives, but instead store data using electronic memory called RAM and ROM. Data stored with these type of memory can be lost if the device loses power. To prevent this loss, PDAs contain batteries, which keep the device supplied with a small amount of power at all times. In order to ensure that no data is lost, PDA batteries must be recharged periodically.<sup>13</sup> This recharging is done on a rotating basis inside the secure data room by outside counsel staff.

---

<sup>13</sup>A small number of the older devices run on batteries that cannot be recharged. For these devices, the batteries are simply replaced with new batteries as needed.



It is not necessary to turn on a PDA in order to recharge its battery. PDAs do not change custody during this procedure.

Outside Houston, storage and security for machines and removable media that contain electronic files is similar to procedures for devices that contain e-mail. Transportation, too, is accomplished using the same methods. Original media may be transported only by ground transportation, accompanied by a DPW or Decision Strategies employee, but copies of media may be transported by Federal Express.

#### **D. Analysis**

##### **1. File Servers and Personal Computers**

Analysis of file servers and personal computers is being conducted by ASR Data Acquisition and Analysis, LLC. Analysis of these devices has four steps. First, the data must be acquired in a manner that does not alter the data itself. Merely turning on a computer normally alters its data. In order to avoid this alteration, ASR uses a method of copying that is non-invasive. Second, the copy must be authenticated in order to ensure that the copy exactly matches the original. These two steps produce an image of the data called an "authenticated bit-image copy." Copying in this manner preserves the forensic integrity of the medium and its copy. To date, authentic bit-image copies have been produced for about 250 personal computers, plus one server. These copies represent approximately 3.5 terabytes of data, or the equivalent of about one billion sheets of printed paper. ASR is in the process of producing authenticated bit-image copies for other servers, as well as for additional personal computers

and drives collected more recently. ASR will continue to produce authenticated bit-level copies for additional machines as they are collected.

The third step in the analysis is to actually observe the copied data. Two principal types of electronic files reside on servers and personal computers: active files and deleted files. Active files are the ones that an ordinary user can see on a device. Deleted files, as the name suggests, are no longer available to the user. Of the two types, active files are easy to observe. Some of the deleted files are relatively simple to recover, while others require a full forensic treatment. Full forensics might include: detection of file fragments; analysis of unallocated space; analysis of "pointers" to files, such as desktop shortcuts; examination of Microsoft Windows registries; detection of whether file-wiping software was used; analysis of machine usage through log files and the like; analysis of Microsoft Windows swap files for virtual memory; and analysis of print spoolers. The fourth and final step is to archive the data in a storable form.

At the moment, ASR is concentrating on active files as well as deleted files that are relatively easy to recover. For the deleted files, ASR is recovering not only the contents of the file, but also the date of deletion when possible. ASR is passing the results to Ibis, which is transforming the data into TIFF format and transferring it to New York for review by counsel. Going forward, ASR plans to continue analysis of active files and easily-recoverable deleted files for the remaining servers and personal computers. It will also begin performing full forensics. Full forensics will not necessarily be performed on every disk, but only where there is some specific reason to do so.

ASR will also be performing analysis on PDAs. Active data on Palm Pilots can be copied, authenticated, extracted and archived in a manner similar to servers and personal computers — except that PDAs must be turned on in order to extract data. That data can then be compared to synchronization records on each user's personal computer.

## 2. File Server Backup Tapes

Ibis is currently conducting the analysis of file server backup tapes. Analysis of file server backup tapes, like analysis of e-mail server backup tapes, proceeds in three steps. First, the tape's electronic label is read in order to determine the server and the backup date. Second, the tape is scanned to create an index of its contents. Third, the tape is restored so those contents can actually be read. During the restore process, two copies are made. One copy is made on another backup tape. A second copy is written to a PC hard drive.

Currently, Ibis is performing all three steps of analysis for some of the backup tapes that cover two servers. Ibis has also completed a preliminary analysis for one server in order to verify its relationship to Enron and is in the process of performing the same relevance analysis for another.

For relevant servers, Ibis will then perform an analysis to detect and restore deleted electronic files. The plan going forward is to perform a differential comparison of file server backup tapes that is similar to the one in progress for e-mail server backup tapes. This differential analysis will reveal whether files were deleted between selected dates. The deleted files will then be restored and transferred to New York, where attorneys will determine whether they are related to the Enron engagement and whether copies in other locations or forms were

retained. The same differential analysis will then be performed for other servers, if initial review shows the presence of relevant material.

Finally, analysis of both existing and deleted files will be extended to the thousands of tapes from remaining servers. The entire process will take a matter of months or longer. In the near future, the restoration of server backup tapes will be assumed by Computer Conversions.

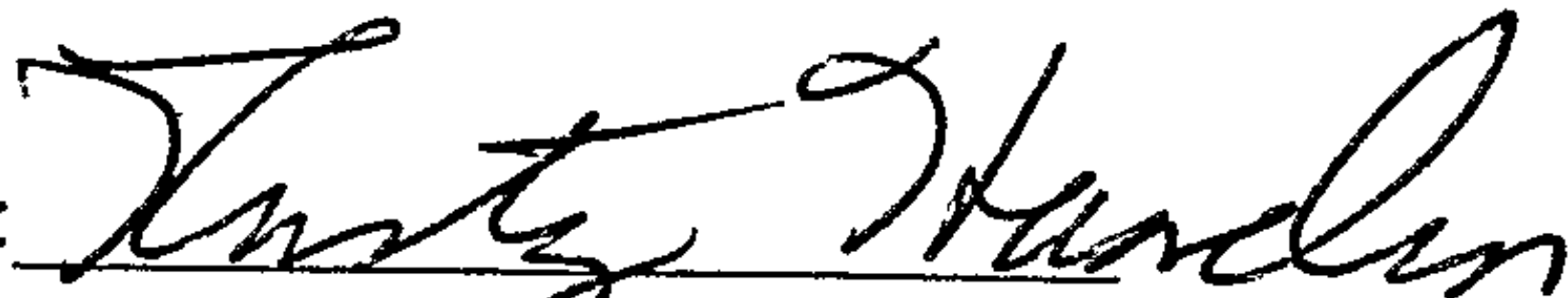
### 3. Removable Media

Analysis of removable media is also in progress. Currently, Ibis has created authenticated bit-image copies of approximately 400 of the removable media. For those media, it has also completed the process of converting active files to reviewable (TIFF) format and sending them to outside counsel in New York. Approximately 3,700 active files were recovered from removable media, and about 183,000 TIFF images of printable pages have been sent to New York for the same type of review noted above. For deleted files, Ibis plans to perform forensic restorations.



Dated: Houston, Texas  
February 12, 2002

Respectfully Submitted,

By: 

Rusty Hardin

State Bar No. 08972800

S.D. Tex. I.D. No. 19424

1201 Louisiana, Suite 330

Houston, Texas 77022-5809

(713) 652-9000

(713) 652-9800 facsimile

Of Counsel:

Andrew Ramzel

Rusty Hardin & Associates, P.C.

1201 Louisiana, Suite 330

Houston, Texas 77022-5809

Daniel Kolb

Michael Carroll

Sharon Katz

Davis Polk & Wardwell

450 Lexington Avenue

New York, New York 10017

(212) 450-4000

(212) 450-4800 facsimile

Attorneys for Defendant Arthur Andersen, LLP

CERTIFICATE OF SERVICE

I hereby certify that on this 12<sup>th</sup> day of February, 2002, that I caused the foregoing Report of Arthur Andersen, LLP on Document Identification, Collection, Restoration, and Retention to be served on the following counsel by first class mail:

Billy Shepherd  
Cruse, Scott, Henderson & Allen,  
L.L.P.  
600 Travis, Suite 3900  
Houston, TX 77002-1720  
713-650-6600  
713-650-1720 (fax)  
*Counsel for D. Stephen Goddard,  
Jr.*

Michael Warden  
Luisa Caro  
Sidley Austin Brown & Wood LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
202-736-8180  
202-736-8711 (fax)  
*Counsel for D. Stephen Goddard,  
Jr.*

Barry G. Flynn  
Law Office of Barry G. Flynn, P.C.  
1300 Post Oak Blvd. #750  
Houston, TX 77056  
713-840-7474  
713-840-0311 (fax)  
*Counsel for David Duncan*

James E. Coleman, Jr.  
Diane M. Sumoski  
Carrington Coleman et al.  
200 Crescent Ct, Ste. 1500  
Dallas, TX 75201  
214-855-3000  
214-855-1333 (f)  
*Counsel for Kenneth L. Lay*

Bruce Hiler  
Robert M. Stern  
O'Melveny & Myers, LLP  
555 13th Street, N.W., Suite 500 W  
Washington, DC 20004  
202-383-5328  
202-383-5414 (fax)  
*Counsel for Jeff Skilling*

Richard Bruce Drubel, Jr.  
Boies Schiller et al.  
26 S Main St  
Hanover, NH 03755  
603-643-9090  
603-643-9010 (fax)  
*Counsel for Andrew S. Fastow*

Craig Smyser  
Smyser Kaplan & Veselka LLP  
700 Louisiana, Suite 2300  
Houston, TX 77002  
713-221-2330  
713-221-2320 (fax)  
*Counsel for Andrew S. Fastow*

Jacks C. Nickens  
Paul D. Flack  
Nickens, Lawless & Flack, L.L.P.  
1000 Louisiana, Suite 5360  
Houston, TX 77002  
713-571-9191  
713-571-9652 (fax)  
*Counsel for Officers: Richard A.  
Causey (Chief Accounting Officer)  
and Richard B. Buy (Chief Risk  
Officer)*

John J. McKetta, III  
Helen Currie Foster  
Graves, Dougherty, Hearon &  
Moody  
515 Congress Ave., Ste. 2300  
Austin, TX 78701  
512-480-5600  
512-478-1976 (fax)  
*Counsel for Rebecca Mark-  
Jusbasche*

H. Bruce Golden  
Randall C. Owens  
Golden & Owens LLP  
1221 McKinney St., Ste. 3600  
Houston, TX 77010-2010  
713-223-2600  
713-223-5002 (fax)  
*Counsel for John A. Urquhart*

Zachary W.L. Wright  
Tonkon Torp, L.L.P.  
1600 Pioneer Tower, 888 S.W.  
Fifth Avenue  
Portland, OR 97204-2099  
503-221-1440  
503-274-8779 (fax)  
*Counsel for Ken L. Harrison*

J. Clifford Gunter, III  
Thomas F. Hetherington  
Abby Sullivan  
Bracewell & Patterson, LLP  
711 Louisiana, Suite 2900  
Houston, TX 77002  
713-223-2900  
713-221-1212 (fax)  
*Counsel for James V. Derrick, Jr.*

Stephen D. Susman  
Kenneth Marks  
Susman Godfrey  
1000 Louisiana, Ste. 5100  
Houston, TX 77002-5096  
713-651-9366  
713-654-6670 (fax)  
***Counsel for Enron Corp.***

Eric J.R. Nichols  
Beck, Redden & Secrest  
4500 One Houston Center  
1221 McKinney  
Houston, Texas 77010-2010  
713-951-3700  
713-951-3720 (fax)  
***Counsel for Michael Kopper***

Robin C. Gibbs  
Kathy D. Patrick  
Robert J. Madden  
Jeremy Doyle  
Gibbs & Bruns, L.L.P.  
1100 Louisiana, Ste. 5300  
Houston, TX 77002  
713-650-8805  
713-750-0903 (fax)  
***Counsel for Outside Directors:***  
***Robert K. Jaedicke, Ronnie C.***  
***Chan, Joe C. Foy, John Wakeham,***  
***Wendy L. Gramm, John***  
***Mendelson, Paulo V. Ferraz***  
***Pereira, Robert A. Belfer, Norman***  
***P. Blake, Jr., John H. Duncan,***  
***Charles A. Lemaistre, Frank***  
***Savage, Herbert S. Winokur, Jr.,***  
***Jerome J. Meyer, and Charls***  
***Walker***

Tom A. Cunningham  
Richard J. Zook  
Cunningham, Darlow, et al  
600 Travis, Suite 1700  
Houston, TX 77002  
713-659-5522  
713-255-5555 (f)

George M. Fleming  
Gregory Sean Jez  
Fleming & Associates  
1330 Post Oak Blvd, Suite 3030  
Houston, TX 77056-3019  
713-621-7944  
713-621-9638 (f)

Thomas E. Bilek  
Hoeffner & Bilek, LLP  
440 Louisiana, Suite 720  
Houston, TX 77002-1634  
713-227-7720  
713-227-9404 (f)

David R. Scott  
Neil Rothstein  
Scott & Scott LLC  
108 Norwich Ave, Suite 1700  
Colchester, CT 06415  
860-537-3818  
860-537-4432 (f)

Roger B. Greenberg  
Schwartz, Junell, Campbell &  
Oathout, LLP  
Two Houston Center  
909 Fannin, Suite 2000  
Houston, TX 77010  
713-752-0017  
713-752-0327 (f)

Jeffrey B. Kaiser  
Kaiser & May, L.L.P.  
1440 Lyric Centre  
440 Louisiana  
Houston, Texas 77002-1639  
713-227-3050  
713-227-0488 (f)

William S. Lerach  
John A. Lowther  
Alexandra S. Bernay  
Milberg Weiss Bershad  
Hynes & Lerach LLP  
401 B Street, Suite 1700  
San Diego, CA 92101  
619-231-1058  
619-231-7423 (f)

Melvyn I. Weiss  
Steven G. Schulman  
Milberg Weiss Bershad  
Hynes & Lerach LLP  
One Pennsylvania Plaza  
New York, NY 10119-1065  
212-594-5300  
212-868-1229 (f)

James D. Baskin, III  
Baskin Bennett  
919 Congress Avenue, Suite 1000  
Austin, TX 78701-2508  
512-381-6300  
512-322-9280 (f)

Robin L. Harrison  
Campbell Harrison & Dagley  
909 Fannin, Suite 4000  
Houston, TX 77010  
713-752-2332  
713-752-2330 (f)

R. Douglas Dalton  
Ron Kilgard  
Dalton Gotto Samson & Kilgard  
3101 N. Central Ave, Suite 900  
Phoenix, AZ 85012-2600  
602-248-0088  
602-248-2822 (f)

Jack E. McGehee  
McGehee & Pianelli, LLP  
1225 N. Loop W., Suite 810  
Houston, TX 77008  
713-864-4000  
713-868-9393 (f)

Richard Frankel  
Hackerman Peterson et al  
1122 Bissonnet  
Houston, TX 77005  
713-528-2500  
713-528-2509 (f)



Robert H. Fritz  
Fritz Law Firm  
330 T.C.Jester Blvd.  
Houston, TX 77007  
713-869-2000  
713-869-3850 (f)

Roger Greenberg  
Schwartz Junell  
909 Fannin, Suite 2000  
Houston, TX 77010  
713-752-0017  
713-752-0327 (F)

Claudia Frost  
Slusser & Frost  
333 Clay St., Suite 4849  
Houston, Texas 77002  
713-860-3300  
713-860-3333(f)

Robert C. Finkel  
Wolf, Popper, LLP  
12<sup>th</sup> Floor Library  
845 Third Avenue  
New York, NY 10022-6601  
212-759-4600  
212-486-2093 (f)

Michael Sydow  
Sydow Kormanik  
1111 Bagby, Suite 4650  
Houston, TX 77002  
713-654-4650  
713-752-2199 (f)

Fred E. Stoops, Sr.  
Richardson, Stoops et al  
The Richardson Bldg  
6555 South Lewis, Suite 200  
Tulsa, OK 74136  
918-492-7674  
918-493-1925 (f)

Steven E. Cauley  
Cauley, Geller, Bowman & Coates  
P. O. Box 25438  
Little Rock, AR 72221-5438  
501-312-8500  
501-312-8505 (f)

Bernard Gross  
Deborah R. Gross  
Law Offices of Bernard M. Gross,  
P.C.  
1515 Locust Street, 2<sup>nd</sup> Floor  
Philadelphia, PA 19102  
215-561-3600  
215-561-3000 (f)

Eli Gottesdiener  
Gottesdiener Law Firm  
3901 Yuma Street NW  
Washington, D.C. 20016  
202-243-1000  
202-537-1989 (f)

Michael D. Donovan  
Donovan Searles, LLC  
1845 Walnut Street, Suite 1100  
Philadelphia, PA 19103  
215-732-6067  
215-732-8060 (f)

Jeffrey Block  
Glen DeValerio  
Michael Pucillo  
Wendy Zoberman  
Berman, DeValerio & Pease, LLP  
577 Gregory Lane  
Devon, PA 19333  
610-695-9007  
610-695-9023 (f)

Steve W. Berman  
Hagens Berman, LLP  
1301 Fifth Avenue, Suite 2900  
Seattle, WA 98101  
206-623-7292  
206-623-0594 (f)

Robert B. Weintraub  
Jeffrey G. Smith  
Wolf Haldenstein Adler Freeman &  
Herz  
270 Madison Avenue  
New York, NY 10016  
212-545-4600  
212-545-4653 (f)

John G. Emerson, Jr.  
The Emerson Firm  
830 Apollo Lane  
Houston, TX 77058  
281-488-8854  
281-488-8867(f)

Lynn Lincoln Sarko  
Keller Rohrback  
1201 Third Avenue, Suite 3200  
Seattle, WA 98101-3052  
206-623-1900  
206-623-3384 (f)

Richard M. Frankel  
Hackerman Frankel & Madela  
1122 Bissonnet  
Houston, TX 77005  
713-528-2500  
713-528-2509 (f)

Frederic S. Fox  
Kaplan Fox & Kilsheimer, LLP  
805 Third Ave, 22<sup>nd</sup> Floor  
New York, NY 10022  
212-687-1980  
212-687-7714 (f)

James E. Wren, III  
Williams, Pattillo, Squires & Wren,  
L.L.P.  
Bridgeview Center, 2<sup>nd</sup> Floor  
7901 Fish Pond Road  
Waco, TX 76710  
254-752-9966  
254-741-6300 (f)

Thomas W. Sankey  
Sankey & Luck, LLP  
600 Travis Street, Suite 6200  
Houston, TX 77002  
713-224-1007  
713-223-7737 (f)

Paul F. Bennett  
Solomon B. Cera  
Gold Bennett Cera & Sidener, LLP  
595 Market Street, Suite 2300  
San Francisco, CA 94105-2835  
415-777-2230  
415-777-5189 (f)



Sherrie R. Savett  
Berger & Montague  
1622 Locust Street  
Philadelphia, PA 19103  
215-875-3000  
215-875-5715 (f)

Richard M. Heimann  
James M. Finberg  
Melanie M. Piech  
Lieff, Cabraser, Heimann &  
Bernstein, LLP  
Embarcadero Center West  
275 Battery Street, 30<sup>th</sup> Floor  
San Francisco, CA 94111-3339  
415-956-1000  
415-956-1008 (f)

Stephen Lowey  
Neil L. Selinger  
David C. Harrison  
William J. Ban  
Lowey, Dannenberg, Bemporad &  
Selinger, P.C.  
The Gateway  
One North Lexington Avenue, 11<sup>th</sup>  
Floor  
White Plains, NY 10601-1714  
914-997-0500  
914-997-0035 (f)

Charles R. Parker  
John Roberson  
Hill, Parker & Roberson, LLP  
5300 Memorial Drive, Suite 700  
Houston, TX 77007-8292  
713-868-5581  
713-868-1275 (f)

Glen DeValerio  
Jeffrey C. Block  
Michael G. Lange  
Michael T. Matraia  
N. Nancy Ghabai  
Berman, DeValerio Pease, et al  
One Liberty Square  
Boston, MA 02109  
617-542-8300  
617-542-1194 (f)

Martin D. Chitwood  
Jeffrey H. Konis  
Chitwood & Harley  
2900 Promenade II  
1230 Peachtree Street, N.E.  
Atlanta, GA 30309-3575  
404-873-3900  
404-876-4476 (f)

Damon Young  
Young, Pickett & Lee  
4122 Texas Blvd  
Texarkana, TX 75503  
903-794-1303  
903-792-5098(f)

Andrew J. Entwistle  
Vincent R. Capucci  
Catherine A. Torell  
Johnston de Forest Whitman, Jr.  
Entwistle & Cappucci, LLP  
299 Park Avenue, 14<sup>th</sup> Floor  
New York, NY 10171  
212-894-7200  
212-894-7273 (f)

Robert I. Harwood  
Frederick W. Gerkins, III  
Wechsler Harwood Halebian &  
Feffer, LLP  
488 Madison Avenue, 8<sup>th</sup> Floor  
New York, NY 10022-5702  
212-935-7400  
212-753-3630 (f)

Laurence D. King  
Kaplan Fox & Kilsheimer, LLP  
100 Pine Street, 26<sup>th</sup> Floor  
San Francisco, CA 94111  
415-336-1238  
415-677-1233 (f)

Joseph J. Tabacco, Jr.  
Berman DeValerio Pease Tabacco  
Burt & Pucillo  
425 California Street, Suite 2025  
San Francisco, CA 94104  
415-433-3200  
415-433-6382 (f)

John Grayson  
Grayson & Hovenkamp  
1221 McKinney, Ste. 1000  
Houston, TX 77002  
713-739-0058  
713-739-0059 (f)

R. Paul Yetter  
Yetter & Warden, LLP  
600 Travis, Suite 3800  
Houston, TX 77002  
713-238-2000  
713-238-2002 (f)

Michael J. Pucillo  
Wendy H. Zoberman  
Berman DeValerio Pease, et al  
515 North Flagler Drive  
Northbridge Centre, Suite 1701  
West Palm Beach, FL 33401  
561-835-9400  
561-835-0322 (f)

Blake Tartt  
Beirne, Maynard & Parsons, LLP  
1300 Post Oak Blvd.  
Houston, Texas 77056-3000  
713-623-0887  
713-960-1527(f)

Michael Pucillo  
Burt & Pucillo  
515 N. Flagler Dr.  
Suite 1701  
West Palm Beach, FL 33401  
561-835-9400

Ira Press  
Kirby McInerney  
830 Third Ave  
10<sup>th</sup> Floor  
New York, NY 10022  
212-371-6600

William Federman  
Dreier Baritz  
120 N Robinson  
Suite 2720  
Oklahoma City, OK 73102  
405-235-1560  
405-239-2112 (F)

Sidney Liebesman  
Grant & Eisenhofer  
1220 N Market St.  
Suite 500  
Wilmington, DE 19801-2599  
302-622-7000  
302-622-7100 (F)

Theodore Anderson  
Kilgore & Kilgore  
3131 McKinney Ave  
LB 103  
Dallas, TX 75204-2471  
214-969-9099  
214-953-0133 (F)

David Mattax  
Office of Attorney General  
P.O. Box 12548  
Austin, TX 78711-2548  
512-463-2018  
512-477-2348 (F)

Jonathan Plasse  
Goodkind Labaton  
100 Park Ave  
12<sup>th</sup> Floor  
New York, NY 10017  
212-907-0700

Joseph Albert McDermott, III  
Attorney at Law  
2929 Allen Pky  
Suite 2555  
Houston, TX 77019  
713-527-9190

Sean Greenwood  
Attorney at Law  
910 Travis  
Suite 2020  
Houston, TX 77002  
713-650-1200  
713-650-1400 (F)

Saul Roffe  
Sirota & Sirota LLP  
110 Wall St  
New York, NY 10005  
212-425-9055  
212-425-9093 (F)

Joe Whatley  
Whatley Drake LLC  
2323 2<sup>nd</sup> Ave N  
Suite 1100  
Birmingham, AL 35203-4601  
205-328-9576  
205-328-9669 (F)

Dr. Bonnie Linden  
1226 West Broadway  
P O Box 114  
Hewlett, NY 11557  
516-295-7906  
516-295-1975 (F)

Charles Richards, Jr  
Richards Layton  
P O Box 551  
Wilmington, DE 19899  
302-651-7738

Paul Thomas Warner  
Reich & Binstock  
4265 San Felipe, Suite 1000  
Houston, TX 77027-0001  
713-622-7271  
713-623-8724 (F)

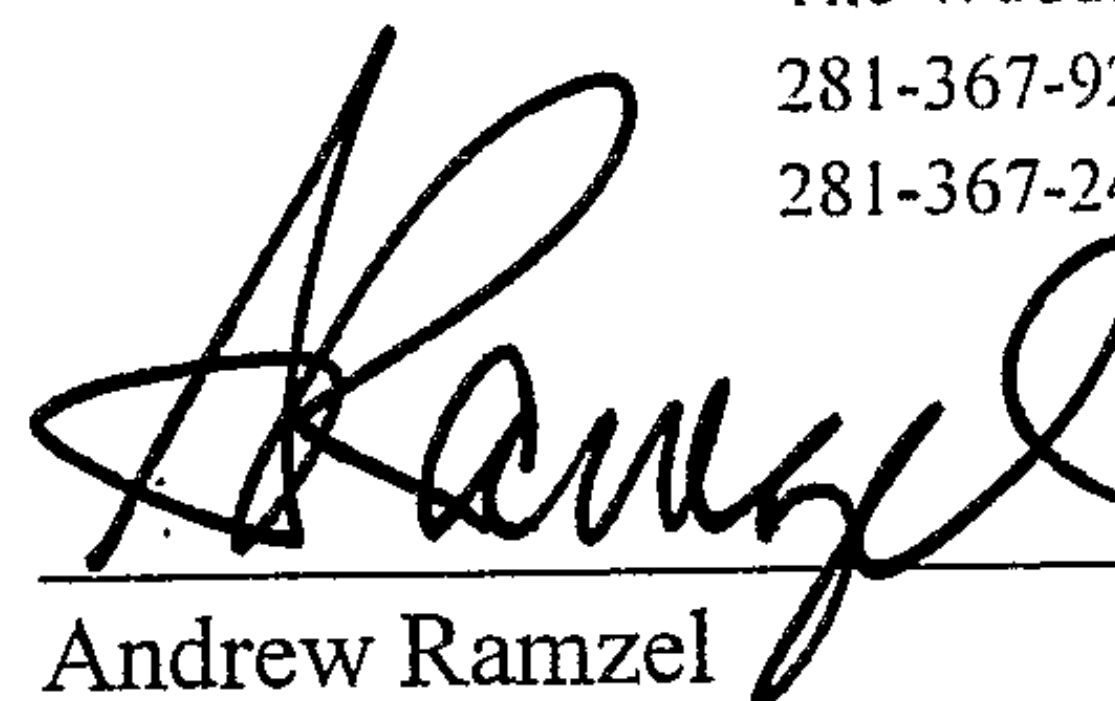
Charles King, III  
King & Pennington  
711 Louisiana  
Suite 3100  
Houston, TX 77002-2720  
713-225-8400  
713-225-8488 (F)

Don Sampen  
Illinois Assistant Attorney General  
100 W Randolph  
13<sup>th</sup> Floor  
Chicago, IL 60601  
312-814-6141

Randy McClanahan  
McClanahan & Clearman  
700 Louisiana  
Suite 4100  
Houston, TX 77002  
713-223-2005  
713-223-3664 (F)

Richard Norman  
Douglas & Norman  
1301 McKinney  
Suite 3500  
Houston, TX 77010  
713-651-1771  
713-651-1775 (F)

Frank Morgan  
Attorney at Law  
1776 Woodstead Ct  
Suite 228  
The Woodlands, TX 77380  
281-367-9200  
281-367-2453 (F)

  
Andrew Ramzel



---

---



# Decision Strategies

A UNIT OF SPX CORPORATION

**Decision Strategies has seventeen years of proven capability handling complex and challenging investigative, private intelligence and security assignments worldwide. The firm specializes in all aspects of corporate, criminal and financial investigations, background and due diligence inquiries, security audits, protecting proprietary information and in gathering litigation intelligence. Decision Strategies' clients include corporations, leading law firms, financial institutions, government agencies, foreign governments and businesses and private individuals. Decision Strategies has built its international reputation by providing discreet, responsive and cost effective service**

## **COMPLIANCE PROGRAMS & MONITORING**

Corporations and individuals can protect themselves by establishing well-functioning and professional compliance programs including education and investigation resolution.

Development and Implementation of Compliance Programs  
Assessment of Effectiveness of Existing Compliance Programs  
Interaction with Regulatory Agencies  
Independent Private Sector Inspector General (IPSIG)

## **DIGITAL SECURITY & INVESTIGATIONS**

Expertise in the digital world has become essential to understanding and negotiating the constantly changing legal, investigative and security fields. The Digital Security and Investigations Group positions our clients to leverage those changes to their advantage by providing experience, insight and intelligence in a variety of digital disciplines including:

Digital & Computer Investigations  
Digital Security  
Electronic Discovery Management  
IT Due Diligence  
Expert Witness Testimony  
Consulting Services  
Specialty & Custom Services

## **CORPORATE INVESTIGATIONS**

In today's competitive global business environment, corporations and the law firms that represent them need timely and accurate information to prepare for and manage corporate investigations. These include:

Anti-Corruption Programs  
Due Diligence  
Employment Investigations  
Workplace Disputes  
Sexual Harassment & Discrimination  
Information Leaks  
Financial Fraud & Corporate Corruption  
Environmental Violations



## EXHIBIT A

### INTELLECTUAL PROPERTY PROTECTION

Decision Strategies has discovered crucial evidence in many proprietary information cases. Our program includes developing and implementing proprietary information protection policies, and detecting and combating trademark, patent and copyright infringements.

### RISK MANAGEMENT

In our business and professional lives, a "surprise" is rarely good news. Decision Strategies is in the surprise reduction and preparedness business. We combine numerous disciplines to take a broad view of human failings and of deliberate and premeditated attacks on you and your company. Risk management services include:

- Due Diligence
- Money Laundering Detection & Protection
- Anticounterfeiting & Gray Market Programs
- Fraud & Corruption Control
- Independent Private Sector Inspector General (IPSIG)

### SECURITY SERVICES

Advanced planning and experienced know-how help to reduce and manage the worst possible security threats. Our security services include:

- Managing Partner Protection Plan
- Kidnap & Ransom Response & Deterrence
- Political Risk Assessment
- Travel Security



## **EXHIBIT B**

CTEC (Cypress Technology and E-Business Center) is Andersen's 40,000-square foot technology center located in Cypress, California. CTEC is staffed with experienced professionals and equipped with advanced network and information systems technology.

CTEC specializes in serving both corporate law departments and law firms by providing discovery management solutions. CTEC combines the full spectrum of document/data management with litigation experience, technology infrastructure, and IT support. CTEC assists clients in managing their data more strategically and effectively.

### **CTEC Services Include:**

- Discovery information management
- Document and data conversion (scanning, coding, OCR etc.)
- Electronic data discovery
- Transactional processing and database design
- Data and value mining services
- IT services and outsourcing
- Web solutions

### **The CTEC Team Includes:**

#### **Client Support Specialists**

Experienced legal industry experts, attorneys and paralegals, who assist clients with litigation support every day understanding how the legal and technology pieces join together.

#### **Database Specialists and Software Developers**

Experienced professionals with expertise in designing, creating and implementing powerful database solutions to manage complex legal, economic, and financial data matters.

#### **Systems & Network Engineers**

Experienced and credentialed systems and network engineers with years of industry experience specializing in network design, implementation, and support, utilizing industry-standard hardware and software solutions.



## THE CTEC FACILITY

- **Infrastructure**

The CTEC network consists of state-of-the-art and industry standard servers, routers, firewalls, network infrastructure and operating systems, with the capacity to expand to meet even the most challenging client needs. In the event of a power outage, CTEC has a redundant power supply system to provide uninterrupted power. Help desk support is also available 24/7.

- **Security**

CTEC is equipped with motion sensors, heat sensors, laser sensors, and cameras to monitor the facility. Badge readers, numeric keypads and hand-geometry readers keep doors secure from unauthorized access. A site scanning, monitoring and fire suppression system is in place to detect any potential water or fire damage.

- **Seismic bracing**

All server racks are seismically braced based on zone 4 seismic codes.

- **Backup & disaster recovery**

The entire system is backed up nightly by a high-speed tape backup system, with backup tapes stored off-site at a secure data storage center.

## REPRESENTATIVE ENGAGEMENTS

### Multinational Consumer Products Company

#### Challenge

Manage more than 20 million pages of documents in response to multiple state, federal and international lawsuits. Address the business and legal issues and mitigate the risks by implementing the right processes and deploying key technology tools.

#### Solution

Teamed with key stakeholders to develop the strategy for establishing processes and leveraging support technology tools. Designed and deployed strategic information management systems to collect, organize and manage more than 20 million pages of relevant documents. This enabled access by more than 700 users in 20 locations throughout the United States and other countries. Established both a private and public network to search and distribute responsive data housed in a central repository.



## **National Insurance Company**

### **Challenge**

In-house legal counsel needed to track the history of document productions across jurisdictions, cases, and core services. Create an enterprise document management system so that in-house legal counsel could participate in the management of cases in conjunction with outside legal counsel.

### **Solution**

Our technology team worked with the client to develop and deploy a consistent infrastructure and technology tool, which enabled the headquarters to support both the internal and external accumulation and distribution of over 9 million pages of relevant corporate documents.

## **International High-Tech Manufacturer**

### **Challenge**

Control and maintain a consistent set of procedures and technology solutions for managing business and legal documents internally. Facilitate the exchange of pertinent information on a timely basis between multiple entities across multiple sites. Mitigate risk and exposure through proper management of the company's intellectual property.

### **Solution**

Implemented a scaleable document management solution to process and distribute information across four key sites and among 30 users. Provided an integrated document processing and repository service for the client.

## **Major Oil and Gas Company**

### **Challenge**

Collect and organize approximately two million documents from various locations for review, scanning and coding. Organize 12 outside counsel firms to work together in reviewing, retrieving and producing the documents as necessary.

### **Solution**

Worked with our ultimate client to set up a process for the attorney review of documents. Established protocols across the different outside counsels so the review happened in a structured, organized manner. Established key communication channels and implemented technologies to ensure that all parties

were apprised of the current project status and issues. All interested parties were provided system access and training so they could independently search and retrieve documents. Also provided litigation support services to interested parties who did not want to access the system themselves.

## **Municipal Bankruptcy**

### **Challenge**

Locate and extract key facts dispersed over 3.5 million pages of documents, including financial reports, correspondence and legal papers. Assist in the development of a strategy in response to state and federal class action lawsuits with damages of more than \$3 billion.

### **Solution**

Worked with lead legal counsel to develop a centralized image and transactional repository containing vital case information. Built infrastructure that allowed simultaneous access by users across multiple sites.

## **Defense and Aerospace Company**

### **Challenge**

Identify, gather, process, review and exchange more than 2 million pages of documents in response to regulatory and corporate requests for a pending merger. These documents spanned multiple years, resided in numerous sites and existed in various forms.

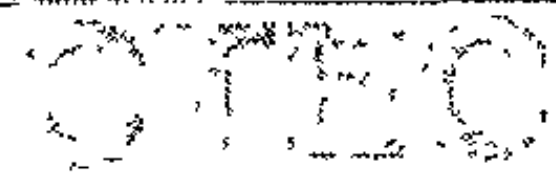
### **Solution**

Provided document-processing services in addition to project management, technology consulting, and software integration consulting. Evaluated and designed the processes and tools to integrate data from various sources and formats. This enabled the client to comply with regulatory and business demands.

## **Global Financial Institution**

### **Challenge**

Gather, organize, analyze, share and manage more than 200 million historical client transactions.



**Cypress Technology and E-Business Center**

**ANDERSEN**

**Solution**

Our team of technology, data acquisition, data migration and data analysis specialists created a data warehouse to house the more than 200 million documents.

( )

( )



EXHIBIT C

**Jay McNally      President & CEO, Ibis Consulting, Inc.**

**College of the Atlantic; Bar Harbor, ME.    1984**  
Bachelor of Arts

**Conley & Hodge      1984-1986**  
*Administrative Manager*  
Responsible for IT systems management and litigation project management.

**Private Consultant    1986-1988**  
*Consultant for Computers in Business*

**Home Shopping Network    1988-1990**  
*Litigation Manager*  
Managed full service litigation facility and staff to meet discovery needs for 3 large lawsuits, and to prepare for and manage 2 month jury trial; analyzed Automatic Call Distribution data against RBOC switch logs.

**Jenner & Block      1990-1991**  
*Administrator/Litigation Support*  
Opened South Florida office for firm; handled paralegal assignments for white collar criminal and civil litigation.

**Document Automation Corporation      1991-1992**  
*Executive Director of Operations*  
Managed scanning and coding staff of 150 people; managed client relations and software development staff; held P&L responsibility for 2 facilities and all non-sales personnel.

**Ibis Consulting, Inc.      1992-Present**  
*President/CEO*  
Worked with and developed programs using Pattern Recognition techniques and Neural/Numerical and statistical techniques to analyze data at issue in litigation;  
Developed risk assessment based on main frame data feeds;  
Worked in forensic analysis of computers;  
Pioneered large scale analysis of e-mail and electronic data.

**Articles Published:**

*Document imaging provides possible answer for managing voluminous data, Vol. 19, Issue 31 MASS High Tech (July 30-August 5, 2001)*

*It May Be Invisible, but Metadata Isn't Insignificant, Vol. XXIV, No.38 Legal Times (Week of September 24, 2001)*

## EXHIBIT C

### **Presentations:**

Large Firm Technology Conference - *Electronic Discovery Issues in Large Scale Litigation* - 1998

East Coast Association of Litigation Support Managers - *Fundamentals of Image Files Format Recognition and Troubleshooting* - 1998

East Coast Litigation Support Managers Electronic Discovery Roundtable - 1999

CLE - Tillinghast Licht & Semonoff - *Discovery of Electronic Data at Issue in Litigation* - 1998

Rhode Island Joint Legislative Committee on Economic Development - *Information Technology Business as a Strategic Economic Driver* - November 2001

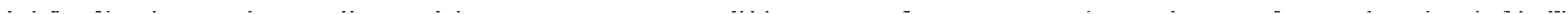
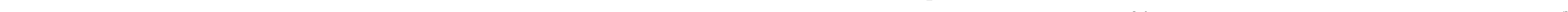
### **Awards and Achievements:**

Rhode Island Technology Council (RITEC), Vice President

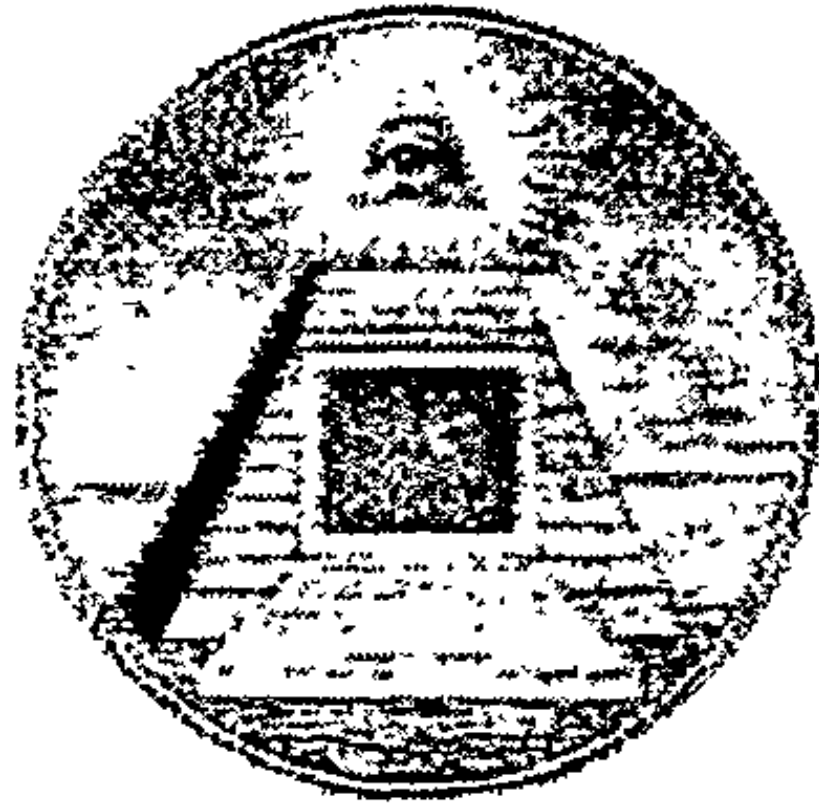
2001 Rhode Island Governor's IT Achievement Award for Outstanding Community Service

2001 Providence Business News "Who's Who In Technology" list

Sole Vision Consultant for Rhode Island's state-of-the art data center



ASR



DATA ACQUISITION  
& ANALYSIS, LLC.

## Andrew S. Rosen

### President Forensic Computer Scientist

As a Forensic Computer Scientist, Andrew Rosen offers unique litigation support services to the Legal, Law Enforcement and Investigative communities.

With over a decade of experience in the recovery of computer data and forensic examination (computer forensics), Rosen regularly provides expert testimony in federal and state courts.

Along with training attorneys and law enforcement officials in computer investigation techniques, Rosen frequently speaks and writes on emerging matters in the field.

In summary, Rosen has a worldwide reputation for developing cutting-edge computer crime investigative tools and is frequently consulted by other professionals in the industry.

### Accolades:

**U.S. Dept of Justice,  
FBI**

"...as a leading authority in the field, your contributions have been significant..." Donald Thompson, Jr.

**U.S. Dept of Justice,  
Criminal Division**

"...your expert assistance and testimony contributed substantially towards our obtaining an optimal result..."  
Joseph S. Gerbasi

**Computer Crime Unit,  
Oregon State Police**

"...gone are the questions, 'how do you know that you didn't change the data?'" Detective Wayne Marney

3505 Cumberland Gap • Cedar Park, Texas 78613  
(512) 918-9227 • FAX 512-918-9393  
[WWW.ASRDATA.COM](http://WWW.ASRDATA.COM) • Email: [info@asrdata.com](mailto:info@asrdata.com)



## **EXPERT WITNESS - TRIAL TESTIMONY**

Expert Witness – *Gyrodatta, Inc. v. Baker Hughes, Inc.*  
Harris County, Texas – 127<sup>th</sup> Judicial District, September, 2001  
Case #2000-40391

Expert Witness - *Colonial Mold, Inc. v. Mancon*  
State of Michigan - County of Macomb, May 2000  
Case #98-1066-CZ

Expert Witness - *Cardinal Health v. Ruscilli Construction*  
Court of Common Pleas, Franklin County, Ohio, June 1999  
Case #99CVH-06-4497

Expert Witness - *United States v. Mulhall*  
United States District Court, Southern District of Florida, March 1999  
Case #96-10014-Cr-ROETTGER

Expert Witness - *Bethesda Softworks v. Seising*  
Montgomery County, Maryland District Court, December 1997  
Case #R96-220659

Expert Witness - *United Tile Corp. v. Ceramic Fiber Fabrications*  
United States District Court, Central District of California, November 1996  
Case #CV 95-1323 WDK

## **EXPERT WITNESS - DEPOSITION TESTIMONY**

Expert Witness – *Lucent Technologies, Inc. v. Kris P. Dehnal, et al*  
277<sup>th</sup> Judicial District Court of Williamson County, Texas - 2000  
Case #00-296-C277

Expert Witness – *Hexagon v. M. Gutterman & Associates, et al.*  
United States District Court, Northern District of Illinois - 1999  
Case #96 C 4356

Expert Witness – *Motorola, Inc. v. Integrated Circuit Systems, Inc.*  
Arizona Superior Court, Maricopa County - 1999  
Case #CV 99-11838

Expert Witness - *Wilson, et al. v. Grout America Inc., et al.*  
United States District Court, District of Arizona - 1998  
Case #CV-98-0884-PHX-SMM

Expert Witness - *Atlantis Plastic Films, Inc. v. Steinhaus*  
Circuit Court of Cook County, Illinois, Chancery Division - 1998  
Case #98 CH 01773

## **PRESENTATIONS AND INSTRUCTIONAL EXPERIENCE**

**Speaker - The Southwest Regional Symposium on Business Continuity, Information Security, and Audit**

ConSec 2001 – Austin, Texas – 9/01

**Speaker - 15th Annual Northwest Computer Technology & Crime Analysis Seminar**

Northwest Computer Technology & Crime Analysis - Sunriver, Oregon - 10/00

**Panelist - Federal Bar Association – Electronic Evidence CLE**

Federal Bar Association 2000 Conference - Cleveland, Ohio – 9/00

**Speaker – Internal Revenue Service, Criminal Investigations Division**

San Diego, California – 8/00 and 9/00

**Panelist - Federal Rules of Civil Procedure - Judicial Advisory Committee**

Hastings College of the Law – San Francisco, California - 3/00

**Speaker - Computer Fraud in the 21st Century**

Baylor University - Waco, Texas - 3/00

**Speaker –Texas State Government Fraud Conference**

Texas State Auditor's office - Austin, Texas - 1/00

**Speaker - 14th Annual Northwest Computer Technology & Crime Analysis Seminar**

Northwest Computer Technology & Crime Analysis - Sunriver, Oregon - 10/99

**Speaker - Texas State Government Fraud Conference**

Texas State Auditor's office - Austin, Texas - 11/98

**Speaker - 13th Annual Northwest Computer Technology & Crime Analysis Seminar**

Northwest Computer Technology & Crime Analysis - Sunriver, Oregon - 10/98

**Speaker - 13th Annual International Symposium on Criminal Justice Issues**

Office of International Criminal Justice - Chicago, Illinois - 8/98

**Speaker - International Association of Computer Investigative Specialists**

International Training Conference - Orlando, Florida - 5/98

**Speaker - Association of Certified Fraud Examiners - Austin, Texas - 1/98**

**Speaker / Instructor - High Tech Criminal Investigator's Association**

Long Beach, California – 9/01

Chicago, Illinois – 9/00

Dallas, Texas - 5/00

El Centro, California - 5/00

San Jose, California - 5/00

Austin, Texas 3/99

New York, New York - 8/98

Boston, Massachusetts - 4/98

San Jose, California - 1/98

Lake Tahoe, California - 10/97

San Jose, California - 9/96

Austin, Texas 11/95

3505 Cumberland Gap • Cedar Park, Texas 78613

(512) 918-9227 • FAX 512-918-9393

WWW.ASRDATA.COM • Email: [info@asrdata.com](mailto:info@asrdata.com)

---

**PRESENTATIONS AND INSTRUCTIONAL EXPERIENCE (cont.)**

**Instructor - FBI Computer Analysis & Response Team**  
Advanced Seizure and Forensic Processing

**Instructor - Canadian Police College**  
Computer Crime Investigative Techniques Training Course (Level II)  
Royal Canadian Mounted Police College - Ottawa, Ontario

**Instructor - United States Department of Energy**  
Computer Crime Investigative Techniques Training Course  
Savannah River Site – Aiken, South Carolina

**Instructor - US Postal Inspectors - Technical Services**  
Computer Crime Investigative Techniques Training Course  
US Postal Services, Lorton, Virginia

**Instructor – Royal Canadian Mounted Police / Canadian Military Police**  
Computer Crime Investigative Techniques Training Course  
Royal Canadian Mounted Police - Halifax, Nova Scotia

**Instructor – George Mason University**  
Computer Crime Investigative Techniques Training Course / GMU 2000  
George Mason University - Fairfax, Virginia

**Instructor – Honolulu Police Department**  
Computer Crime Investigative Techniques Training Course  
Honolulu PD – Honolulu, Hawaii

**Instructor – California P.O.S.T.**  
Computer Crime Investigative Techniques Training Course  
Stockton PD – Stockton, California

**Instructor – Australian Federal Police / New South Wales Police**  
Computer Crime Investigative Techniques Training Course  
New South Wales PD – Sydney, Australia



## PROFESSIONAL EXPERIENCE

**Apple Computer, Inc. - Austin, TX**  
Technical Support Specialist -- Tier II

**March 1994 -- January 1997**

- Troubleshoot and resolve hardware/software/network problems
- Develop, implement, and maintain software tools and information delivery systems
- Perform software evaluation, functional analysis, and compatibility testing

**Amgen, Inc. - Westlake Village, CA**  
MIS Specialist

**September 1993 -- January 1994**

- Develop, implement, and maintain software tools and information delivery systems
- Design and present educational and training materials
- Troubleshoot and resolve software/network problems

**Symantec / Peter Norton Group**  
**Santa Monica, CA**

**November 1992 -- September 1993**

Quality Assurance Engineer/Technical Support Specialist

- Design and develop software and methodology for stress testing software products
- Provide developer support, software evaluation, design and functional analysis
- Hardware/software fault interpretation and resolution
- Specialist in the diagnosis, repair and recovery of disk volumes and file data
- Software acceptance testing, low level disk editing

**McDonnell Douglas, Space Station Division**  
**Huntington Beach, CA**

**June 1992 - November 1992**

Programmer - Systems and Network Analyst

- Develop custom application programs
- Create custom network management utilities
- Configuration and installation of computer, file servers and workstations
- Facilitate transfer of sensitive data

**ASR Consulting Services -- Los Angeles, CA / Austin, TX**  
Programmer / Software Developer / Instructor / Consultant

**July 1984 - Present**

- Develop custom software solutions
- Training and instruction in Forensic Computer Data Analysis
- Data Recovery and Data Discovery
- Expert Witness / Litigation Support





## LEE TYDLASKA

1774 Sunset Rose Court  $\approx$  El Cajon  $\approx$  CA  $\approx$  92019

(800) 328-2911

[leet@computer-conversions.com](mailto:leet@computer-conversions.com)

Lee Tydlaska received his Bachelor of Science degree in Criminal Justice from California State University, Los Angeles in 1976. He currently serves as a board member of the Forensic Consultants Association and is an active member of the High Technology Crime Investigation Association. In October 1994, he became a Certified Business Continuity Planner and currently advises companies regarding the integrity of their computer backup systems.

From 1980 to 1984, he owned and operated Computer Communications, a consulting firm which assisted businesses and individuals transferring data to new systems. In 1984, he founded Computer Conversions, Inc., an internationally recognized data recovery and data conversion services company. As President of Computer Conversions, Lee has assisted thousands of clients by recovering information thought to be permanently lost from damaged backup media.

### Education

1976	B.S. Criminal Justice - Calif. State Univ., Los Angeles
1977	Graduate - San Diego Sheriff's Academy
1994	Certified Business Continuity Planner - Disaster Recovery Institute

### Experience

01/95 – present	National Speaker at Computer Crime Conferences
12/83 – present	President and Founder - Computer Conversions, Inc.  Recognized as a leading expert in data recovery and data conversion. Developed specialized data recovery and data conversion technologies.
1/79 - 12/83	Teletext Technician Time Video Information Service/Southwestern Cable TV
9/76 - 12/78	Deputy Sheriff San Diego County Sheriff's Department

### Expert Testimony

2001	Clements, O'Neil, Pierce Houston, TX
2000	Beemer vs. Lifelike Products

Texas Court #565541999

1999 Krighton & Karim vs Karim

1991 Dilley vs. Allstate Insurance  
California Court # 622403

1984- Present Provided pre-trial evaluation and consultation for various government cases, involving E-mail, computer backup systems and procedural issues.

### **Professional Associations**

Member, Forensic Consultants Association  
Member, High Technology Crime Investigation Association  
Member, Toastmasters

### **References**

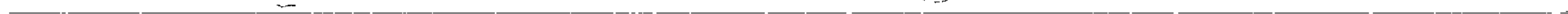
Ovation Data Services, Inc.  
Gregory Servos  
10650 Haddington Dr.  
Houston, TX 77043  
[www.ovationdata.com](http://www.ovationdata.com)  
[gregory.servos@ovationdata.com](mailto:gregory.servos@ovationdata.com)  
(713) 464-1300

Shaffstall Corporation  
Tony Shaffstall  
7901 E. 88<sup>th</sup> St,  
Indianapolis, IN 46256  
[www.shaffstall.com](http://www.shaffstall.com)  
(800) 357-6250

Forensic Consultants Association  
Ralph Godfrey  
R. Godfrey Consulting  
11147 Negley Ave  
San Diego, CA. 92131-1819  
[www.floorspy.com](http://www.floorspy.com)  
[ralph@floorspy.com](mailto:ralph@floorspy.com)  
(858) 695-8174

TLSI Incorporation  
John Wiechman  
123 N. Beltline Road  
Grand Prairie, Texas 75050  
[john@TLSI.net](mailto:john@TLSI.net)  
(800) 465-8574

ARS Consulting Services  
Andrew Rosen  
3505 Cumberland Gap  
Cedar Park, Texas 78613  
[www.io.com/~asrcs/](http://www.io.com/~asrcs/)  
[asrcs@io.com](mailto:asrcs@io.com)  
(512) 918-9227





## EXHIBIT F

### Enron Electronic Data Discovery – Email Processing

#### **Purpose:**

The purpose of this memo is to document the scope, methodology, and procedures performed during CTEC's Enron Electronic Data Discovery process.

#### **Discussion:**

##### Background

CTEC is engaged to perform Electronic Data Discovery (EDD) for selected Andersen employees' that have been associated with the Enron account. The purpose of this discovery is to maintain the chain of custody and build an accurate, historical record of each employee's electronic mail database.

##### Methodology

Andersen performs routine, and as requested non-routine, e-mail server back-ups. The back-up process captures an individual's e-mail account history and freezes it at that point in time. CTEC's reconstruction methodology centers on its ability to capture a historical database back-up at these multiple dates for each of the selected Andersen employees' Lotus Notes e-mail accounts. From this series of individual back-up files, the Lotus Notes' functionality to assign each existing and deleted document (e-mail), and its corresponding attachments, a unique identification number, CTEC can reconstruct the record of e-mail activity.

Lotus Notes assigns every document (e.g., e-mail, calendar entry, to do task, address book entry, etc.) a unique identification number. Through an electronic document ID matching process, CTEC is able to identify each of the unique document identification numbers for every available back-up date and screen them against other periods. As each historical layer is matched against its subsequent layer, CTEC is able to single out documents from duplicates thereby previously deleted documents are now "recovered." The accumulated record of original documents is warehoused in CTEC's database and available for authorized distribution. See the account reconstruction example below.

##### Analysis

Upon compilation of the copy of the original record database CTEC performs specific account activity analysis. Amongst other capabilities, this analysis can identify who received which communication from whom, when each communication was received, the contents of each communication, and, using the Delete Stub identification number, when the communication was deleted.

Due to the individual mailbox owner's ability to control the Delete Stub purge process it is possible for a document to be received, deleted and the delete stub be purged between regularly scheduled back-ups. The mailbox's rolling purge frequency is executed at 1/3 intervals of the selected purge period. For example the default purge cycle is 90 days, hence every 30 days the database purges all delete stubs aged greater than 90 days. The example's opportunity window is 91 days, thus if an individual's back-ups span beyond 91 days the likelihood for exposure increases. However, with each back-up received, the time-gap between back-ups is reduced and the possibility for a document to fall within the window is exponentially reduced. The actual opportunity window is dependent upon the individual's ability to reduce or increase the default time from zero to 9,999 days.

## Enron Electronic Data Discovery – Email Processing

### *Example*

Assume today is the first of June and the task is to reconstruct an individual mailbox database back to the first of January. To illustrate the document recovery process review the following chart and assume that each e-mail database is backed up at the end of the month. If a document (e.g., e-mail, calendar entry, to do list items, address book changes, etc.), with the Lotus Notes Unique Identification Number (LNUIN) of #19, was received in January and retained, the document would be included on the January 31<sup>st</sup> back-up. The document would continue to be backed-up each of the subsequent months until purged from the mailbox database.

If document #19 was kept through January and subsequently deleted in February it will show up in the February Delete Stub log. Again, upon any document's deletion Lotus Notes assigns the document a "Delete Stub". This Delete Stub records the document's deletion date and time, and ties to the original document's LNUIN. This Delete Stub is retained until its purged, as established by the individual mailbox account holder.

To perform the EDD recovery CTEC would obtain a copy of the available back-up records and begin with the most recent, May 31, back-up date. On the chart below, CTEC will use the May back-up database to identify the baseline of documents that existed #1 - #4, those that were deleted during the month, #5 - #12, and deduce that #13 to an unknown total existed sometime in the past. By comparing the LNUINs from the May back-up to the LNUINs on the April back-up, CTEC can obtain copies for documents #5, #6 and #7, confirm that #8 - #12 are from a prior period, and more importantly, use the Delete Stub record to identify the existence of documents #13 and #14. Adding March's LNUINs to the process recovers deleted documents #8 - #11 and identifies the existence of documents #15 - #20. At the time it's unknown what is contained within document #19, nor does CTEC know that #19 is the particular document in question, but its now known that #19 exists like the rest. By repeating this process for each of the available back-up dates, CTEC is able to recover the documents for #1 - #24, including #19 in January, and from the delete stub record know that documents #25 - #32 existed in prior periods.



# Enron Electronic Data Discovery – Email Processing

Doc. ID#	Back-Up Date	Back-Up Date	Back-Up Date	Back-Up Date	Back-Up Date	Original Doc. Master Log
	31-May	30-Apr	31-Mar	28-Feb	31-Jan	Recovered
1						
2						
3						
4						
5	-					
6	-					
7	-					
8	-					
9	-					
10	-					
11	-					
12	-					
13	X					
14	X					
15	X	X				
16	X	X				
17	X	X				
18	X	X				
19	PURGED	PURGED	DELETED	DELETED	DELETED	DELETED
20	X	X				
21	X	X	X			
22	X	X	X			
23	X	X	X			
24	X	X	X			
25	X	X	X			
26		X	X			
27		X	X			
28		X	X			
29		X	X			
30			X			
31			X	X		
32			X	X		
33			X	X		
34			X	X	X	
35				X	X	
36				X	X	
37				X	X	
38				X	X	X
39					X	X
40					X	X
41					X	X
42						X
43						X

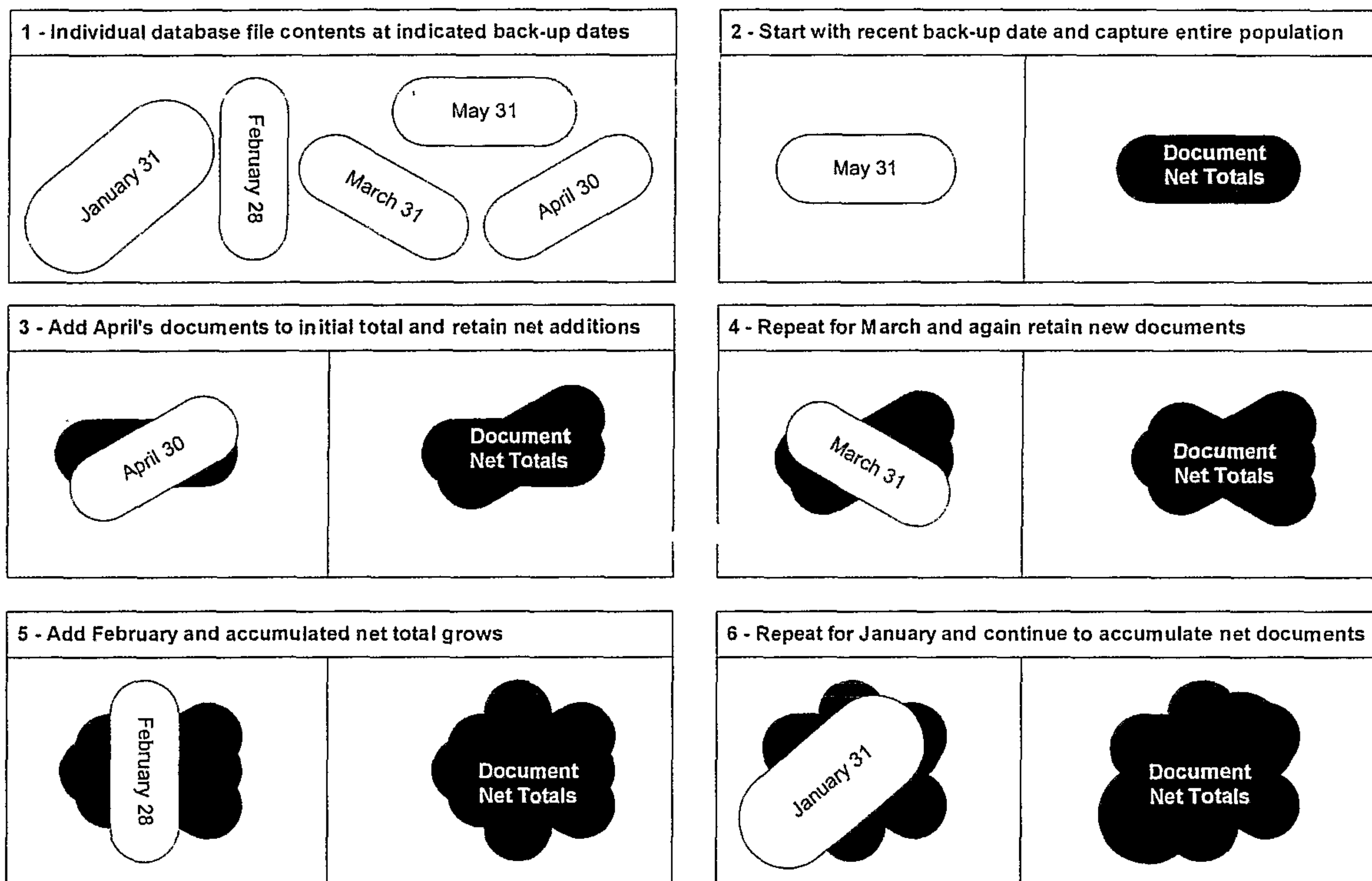
-
X

E-mail exists and has been retrieved  
E-mail Delete Stub exists  
E-mail Delete Stub has been purged

## Enron Electronic Data Discovery – Email Processing

In our example, Document #19 was received in January, backed-up at the end of January and deleted in February whereupon it received a unique Delete Stub identifier. This Delete Stub was then part of the February and March month end back-ups until it was finally purged from the database record in April. CTEC used each back-up to reconstruct an accurate, historical record of the mailbox database by identifying each document per back-up and labeling it as an original or duplicate of an original previously recovered.

By looking at the process as a series of layers it's evident that as you add one on top of the other you're filtering out duplicate LNUINs and only accumulating new documents. Except for documents purged, this layering process recovers all available documents and collectively accumulates them into a single database. The chart below diagrams CTEC's application of each LNUIN layer to the original and building the accumulated LNUIN population.



The process of applying the chart's layers is described below within the Procedures section.



## Enron Electronic Data Discovery – Email Processing

### Procedures

The technical process to support the methodology is a combination of internally developed proprietary analysis tools and off the shelf software. As aforementioned, to maintain the integrity of the EDD process CTEC developed a number of information handling and processing procedures. A designated team strictly follows these procedures to inventory every mailbox received, specifically track its processed status, log its document recovery results and account for its delivery to an authorized recipient. A detailed discussion follows.

#### *Requesting and obtaining individual e-mail account mailboxes*

CTEC uses an excel spreadsheet (\*.xls) as a standardized request form. Each individual's mailbox (\*.nsf) for a specific date is retrieved locally from the source and copied on an available media type. This request form is populated by a technician at the individual's local office and, with a source media back-up copy of the individual's mailbox database, is returned to CTEC for processing. These files are then sent to CTEC and logged upon receipt into the Inventory database (\*.mdb).

#### *Receiving requested e-mail account mailboxes*

CTEC receives both the populated spreadsheet and source media mailbox back-up copy. The spreadsheet information is reconciled to the files received and, as applicable, corrective changes are made. All non-digital types are converted to CD/DVD. Upon completion of the check-in process the source media files are logged into CTEC's EDD inventory database (\*.mdb) and the detailed file information is uploaded from the spreadsheet and matched to the source media.

#### *Staging for processing*

After each \*.nsf file is recorded into the inventory database it is copied to a dedicated and secure network location. Files are moved from the source media to the network drive and the source media is archived to a secure facility. The network drive becomes the electronic master location for all files received. A copy of the file is then captured and staged for processing. The staging process includes documenting the file size along with document and delete stub quantities.

#### *Processing*

CTEC processes each file identically with the only noted exception being an extra step for the November 30, 2001, back-up files whereupon the Delete Stubs are extracted to establish a document deletion timeline.

- Deletion Stub Extraction

Using Notes Peek, a Lotus developed program, CTEC is able to segregate the Delete Stubs from the individual account's mailbox database (\*.nsf) and save this detail in text form (\*.txt). Delete Stubs retain the original document's Lotus Notes Unique Identification Number (LNUIN), the document's fingerprint, and are used later in the process to matched the Delete Stub Identification Number to their corresponding recovered document's LNUIN. This process establishes a document's deletion

## Enron Electronic Data Discovery – Email Processing

timeline. A histogram of the analysis is used to pictorially review activity patterns and identify specific time periods for further review.

- Duplication Analysis

To break down the \*.nsf database into unique and examinable parts a utility is used to parse the individual's mailbox data each document's Field Info (To, From, CC, BCC, Date, Time, Subject, Body, Notes ID, Path, etc.). Concurrently, the process detaches all attached files, grants each a unique identification number, and files the attachments within a designated directory on the CTEC network.

The organized Field Info data is loaded into a SQL database for analysis. The loading process reviews each Field's LNUIN to existing data from the same mailbox owner. Original LNUIN's are captured and loaded into the database, duplicate LNUIN's are identified and disregarded.

- Recovered Document Warehouse

Subsequent to loading the original documents into the SQL database and each of the document's corresponding attachments, the entire file is rasterized and warehoused within CTEC's data warehouse. It's during this "rasterization" process that the \*.nsf file, by individual document (e-mail, calendar entry, to do list items, address book changes, etc.), and its corresponding attachments are reunited by their LNUIN and converted from their original file extension ( i.e. \*.doc, \*.xls, \*.ppt, etc.) to viewable \*.tif images.

To accomplish the rasterization of miscellaneous file attachments, CTEC utilizes the Outside In® Viewer Technology Version 7.1 Active X Control. This allows for a wide array of file types to be printed to \*.tif format. (See attached "Supported File Formats" for details).

- Un-Converted Files

Certain file types do not lend themselves to the rasterization or electronic "printing" process. As such, certain file extensions are automatically excluded from this process. In addition, encrypted files and corrupt files are not converted. All non-rasterized attachments are tracked within the database for reporting purposes. In addition, upon request these files can be provided in their native format for further review.

### *Delivering*

Upon request, data from the document warehouse is extracted in duplicate to digital media. Load files are created based on the requirements of the target system. One copy is sent to the requestor and the second is recorded and stored in CTEC's work papers.

## **Enron Electronic Data Discovery – Email Processing**

- Deletion Stub Analysis

Upon specific request, available date and time Delete Stub information is matched to its corresponding document. The Delete Stub matching process enables the reviewer to analyze the document's retention and disposal record.

### *Documentation & Controls*

The complete EDD process is governed by policies, procedures and established controls. A designated librarian manages the EDD Inventory and corresponding Database. Via the Inventory Database the librarian accounts for each media's receipt, tracks its processing status, records the quantity of documents received and corresponding documents produced, accounts for media physically 'checked-out' of the secure facility, performs routine reconciliation of the Inventory Database to physical media received, adheres to quality assurance reviews, facilitates exception handling protocols and maintains a document deliverable log.